**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 285**

Security Equipment

**Security hardware**

1. What is meant by data integrity?

Data integrity is the assurance that data is accurate and reliable, and is available in a timely manner.

1. Biometrics
   1. Describe biometric security.

Biometric security refers to the use of physical human characteristics, including fingerprints, facial features, or behavioural characteristics such as voice patterns or handwriting. These human characteristics are used to authenticate the user before giving them access to the data.

* 1. Why does it appeal to security managers?

The use of biometrics appeals to security managers as it all but impossible to copy or steal a person’s biometric characteristics, thus making unauthorised access to the any data much harder.

* 1. List the common biometric devices.

The most common biometric devices are:

* Voice recognition: is when a person’s speech is compared with a stored voice pattern, each user must ‘train’ the computer to recognise their voice by repeating several words over and over again.
* Fingerprint recognition: is the use of a fingerprint scanner to scan each small ridge and swirl of a fingerprint, this image is matched with a pre-scanned image of the users finger print (consisting of at least 20 points).
* Hand geometry: in this system the size and layout of the hand is measured and key features are noted, this is able to be matched when the users hand is scanned. (This technology is the predecessor of fingerprint recognition technologies).
* Signature verification: this is when a stored copy of the user’s signature is compared with the signature written on a pressure sensitive tablet, this measures both the pressure and motion used.
* Facial recognition: this technology is used to verify a person’s identity, it uses an 80 point system recognise a person’s face (it verifies elements like the distance between a person’s eyes, chin line or depth of their eye sockets). Facial recognition can match a person standing directly in front of the camera or pick them out from a moving crowd.
* Iris recognition: this system uses a person’s iris to identify them (the iris is one of the most unique features that a person has, and for this it is believed to be one of the most accurate biometric systems available). The scanner checks up to 247 independent points on the iris.
  1. What are the concerns of biometric technology?

The main concern that is associated with biometric technologies is their intrusive nature. But since the prevalence of the threat of terrorism in our society organisations have become more comfortable with the use of biometric technology.

1. Swipe cards
   1. Describe the nature of a swipe card.

Swipe cards are a common type of security device used by many people. They are usually a business-card-sized plastic card with a magnetic strip on one side and the details of the user on the other.

* 1. What is a limitation of the swipe card?

The main limitations of swipe cards are:

* A swipe card is they can be easily damaged by magnetic fields, and
* If stolen a swipe card offers little protection of the owners details from the thief, and with a swipe-card reader the can capture any data on it.

1. Smart cards

Smart cards are more recent developments in technologies that make the smart card. The smart card is much like a swipe card except that it has a microchip imbedded in it tho store and manipulate the user’s data.

1. Security tokens

Security tokens are small devices that are about the size of a key ring which can be used to deal with sensitive information. For example a security token may be used to display a constantly changing authentication code, when a user wants to access this information they have to enter their account name and password, and then the authentication code will be displayed on the security token.

1. Mobile phone secure code
   1. How does this level of authentication work?

This level of authentication works when a security code is sent to the account holder’s mobile phone to authenticate a transaction before it occurs. The account holder needs to log in and enter the code before the transaction can be processed.

**Power protection**

Outline the characteristics of the following:

1. Surge protector

A surge protector is the most basic form of device that protects against electrical damage; this protects electrical equipment against overvoltage caused by a power surge.

1. Uninterruptible power supply, (UPS)

An uninterruptible power supply is better form of protection against power fluctuations. A UPS is a high quality surge protector which is built into the device; it will not only guard against power spikes but also help keep data if there is an undercurrent or complete failure in power.

**Strategies for avoiding system failure, p 288**

1. What is meant by redundancy?

Redundancy means that no part of the system is critical to the overall operation of the system. If there is one part of the system fails there will be another part of the system to ensure that there is no loss of data.

1. What is meant be a fault-tolerant server?

A fault-tolerant server will continue to work even if a piece of the hardware within it has failed, this tolerance is achieved by having multiple components, such as having dual hard drives, motherboards or power transformers running parallel.

1. Redundancy through multiple hard drives or fault-tolerant equipment
   1. Describe how this redundancy works.

Redundancy ensures that there is something in place to keep the system running and to ensure against the loss of data if one piece of the system fails.

* 1. What is meant by RAID technology

RAID technology refers to a popular method for guarding against hard disk failure. It uses an array of inexpensive disks to create redundancy. A RAID protected system sends fragments of data to over several hard drives, so if one hard drive fails the others can piece together the missing data and rebuild the file using error-checking codes.

1. Redundancy through mirrored servers or machines
   1. Why is the RAID solution preferable to this solution?

A mirrored server refers to a server that is copied exactly on to another to create redundancy. A RAID solution is preferred to this system as if there is a failure whilst using the RAID system the user will not know but when using a mirrored system the user will notice when the second server has to be accessed.

**Backup Media**

1. There are a range of options for backup media, what 3 factors should be considered when deciding on which backup media to use?

The three factors to consider when selecting back-up media are:

* The cost of the drive or writer
* The cost of media per GB
* The speed and compatibility

Three categories of backup media:

* Magnetic media
* Optical devices
* Solid-state devices

List the characteristics of the following backup media:

**Magnetic media**

1. hard disk drive

This is an affordable media option to backup files. It is best to have a removal hard disk drive so it can be taken away if there was any form of disaster that posed a threat to it (e.g. a flood or fire), if it is not removable it may be destroyed along with the original. It is also possible to backup to a networked hard drive located offsite.

1. Magnetic tapes

Magnetic tapes are a popular form of media for backing-up files. Magnetic strips are also relatively cheap, but are slow to save and restore files, as the tape must be read an accessed sequentially (i.e. if the file which needed to be restored was at the end of the tape the whole tape must be progressed past until the file needed is reached).

**Optical media**

1. Compact disc

Compact discs are a form of removable media that can hold up to 700MB of data (which is approximately 80 minutes of audio). There are two forms of compact discs CD-Read which cannot be rewritten and CD-RW which can be rewritten.

1. DVD

A DVD, digital versatile disc or digital video disc, has become a popular back-up medium in more recent times, and are able to hold up to 17GB (double sided). Also like CD-ROMs these can come in either non-rewriteable (DVD-R) or rewriteable (DVD-RW)

1. Blu-ray

Blu-ray is a new optical disc format with a capacity of 50GB (dual layer), that was designed to replace the DVD format. The name comes from the blue laser that is used to read the disc, which allows for five times more storage than DVD and also for the storage of high definition films.

**Solid-state drives**

1. USB storage devices

This form of backup media is very popular, they are often small and sold as a key ring that can be transported anywhere. Added to this USB storage devices do not have any moving parts (as their memory is solid state), this means that there is a lower chance of breakdown, and they have the ability to hold up to 256GB of data.

**Online backups**

1. Why do organisations use this form of backup?

Organisations use this form of backup as they can ensure that they work as efficiently and effectively as possible.

1. Describe an enterprise storage system.

An enterprise storage system typically involves the interconnection via a storage network area (SAN), of RAID disks, tapes, CD/DVD-ROM servers, internet backup and other network storage devices.

**Surveillance technology, p 292**

Describe the nature of the following items of surveillance equipment used in offices:

1. Packet sniffers

Packet sniffers are diagnostic tools that monitor the contents of packets being sent across networks. They can be set to filter packets containing certain data elements and copy them to an administrator’s computer for further analysis.

1. Desktop monitoring programs

A desktop monitoring program works by intercepting every action performed on a computer. The program must first be installed on the computer (done easily by the administrator), before a person can see exactly what you are doing on a computer.

1. Log files

Log files are generally files that contain a log of when a certain application was run, also the applications themselves may create log files. Another example of a log file is on a network where all users who log in are put on the logs.

1. Closed-circuit television, (CCTV)

Closed-circuit television consists of a series of cameras that are linked to an internal TV system. This form of surveillance technology is often watched by security guards so they can monitor what people in a certain area are doing.

1. Telephones

So organisations will monitor the telephone usage of employees (generally to ensure that all calls are restricted to the company or business and are not personal). Most employees are given their own extension so it easy to tell how an employee is using their telephone.

1. Audit trails

It is important that any access and modification to files can be traced; do if problems occur it is known who is likely to have caused them. The combination of surveillance technologies allow manager to trace transactions or any other forms of activity on an information system, this is called an audit trail.

**Physical security devices:** List the options for physically securing your data

The options for physically securing data are:

* Lockable disc box
* Storage inside of a safe or specialised room
* Attaching hardware to fixed structures with cables

Darcie Anderson